



King's Research Portal

Document Version
Peer reviewed version

[Link to publication record in King's Research Portal](#)

Citation for published version (APA):

Bochow, B., Holland, O. D., & Katzis, K. (2016). Spectrum Sensing Infrastructure Support for IEEE 1900.6b Sensing-Assisted Spectrum Databases. In *2016 IEEE Conference on Standards for Communications & Networking (CSCN'16)* Institute of Electrical and Electronics Engineers Inc..

Citing this paper

Please note that where the full-text provided on King's Research Portal is the Author Accepted Manuscript or Post-Print version this may differ from the final Published version. If citing, it is advised that you check and use the publisher's definitive version for pagination, volume/issue, and date of publication details. And where the final published version is provided on the Research Portal, if citing you are again advised to check the publisher's website for any subsequent corrections.

General rights

Copyright and moral rights for the publications made accessible in the Research Portal are retained by the authors and/or other copyright owners and it is a condition of accessing publications that users recognize and abide by the legal requirements associated with these rights.

- Users may download and print one copy of any publication from the Research Portal for the purpose of private study or research.
- You may not further distribute the material or use it for any profit-making activity or commercial gain
- You may freely distribute the URL identifying the publication in the Research Portal

Take down policy

If you believe that this document breaches copyright please contact librarypure@kcl.ac.uk providing details, and we will remove access to the work immediately and investigate your claim.

Spectrum Sensing Infrastructure Support for IEEE 1900.6b Sensing-Assisted Spectrum Databases

Bernd Bochow
Next-Generation Network Infrastructures
Fraunhofer FOKUS
Berlin, Germany
bernd.bochow@fokus.fraunhofer.de

Oliver Holland
Centre for Telecommunications Research
King's College London
London, UK
oliver.holland@kcl.ac.uk

Konstantinos Katzis
School of Sciences
European University Cyprus
Nicosia, Cyprus
k.katzis@euc.ac.cy

Abstract— Spectrum databases are increasingly being used, particularly in spectrum sharing mechanisms, but also in realms such as network optimization, novel licensing regimes, and regulatory monitoring, among others. Spectrum databases are often far more effective, reactive, or sometimes even are required to operate, in conjunction with spectrum sensing—especially if their operation requires automation. Given such observations, this paper presents an update on the IEEE 1900.6b standards work on spectrum sensing to support such databases. Specifically, this paper provides an overview of IEEE 1900.6 and the current work towards 1900.6b, pinpointing the latest updates and thoughts on aspects of the system model incorporating spectrum databases, as well as use cases for the standard. It particularly concentrates on some of the more recent developments and challenges that IEEE 1900.6 is addressing for 1900.6b, such as sharing of sensing infrastructures with different client constraints (noting that spectrum databases—the clients—may have very different requirements in terms of measures such as accuracy and reliability), flexibility in the definition of sensing infrastructures, and security requirements, among many others. This paper finishes by presenting some detail on an experimental set-up for an upcoming trial of the IEEE 1900.6 standard as amended with IEEE 1900.6b capabilities, supporting the operation of a spectrum database as a key European showcase.

Keywords—*Spectrum databases, sensing infrastructures, standards.*

I. INTRODUCTION

There are numerous recent developments in the technological scope that point towards the use of (broadly-speaking) spectrum databases to make automated real-time decisions on spectrum sharing. These include Spectrum Access Systems (SASs) in the context of the three-tier 3.5 GHz Citizens' Broadband Radio Service (CBRS) in the US [1], Licensed-Shared Access (LSA) Controllers in the context of LSA in Europe [2], and geolocation databases in the context of TV White Space (TVWS) in the US, UK, Singapore, and elsewhere [3], [4]. There is also increasing drive for Self-Organizing Networks (SONs) and other automated management regimes in the context of increasingly complex, varied and dynamic (for optimal operational reasons) mobile/cellular networks. Such concepts also require spectrum database functionality. Further, the need for regulatory monitoring based around such databases, and other regulatory concepts such as (semi-)automated "light licensing" using databases to keep track of licenses and to assess the appropriateness of applications for licenses based on, e.g., the change in level of interference in the area that would result.

Spectrum sensing in some cases must be combined with such databases, examples being the Environmental Sensing Capability (ESC) feeding the SAS in the US CBRS [1]. In regulatory monitoring capabilities, and likely in other cases such as SON, spectrum sensing assisting such databases might be greatly beneficial. For example, in TVWS, sensing might help to inform or enhance complex propagation information models that the regulator uses to calculate which TV channels can be used where and in some contexts with which allowed EIRP, without violating primary interference thresholds at receivers. In LSA, such sensing might ensure that the 'secondary' usage of the operator's spectrum is not causing more than a threshold of interference, noting that such capabilities might also be used for purposes such as SON in this scenario.

The IEEE 1900.6 working group serves distributed spectrum sensing infrastructures and data structures. Within that scope, work aims to enhance the 1900.6 baseline standard for the purpose of spectrum sensing information to assist spectrum databases, considering different realization options. Consequently, a spectrum database may be an embedded function of a larger system as well as a large distributed spectrum authorization system. This paper outlines some of the current work and objectives towards IEEE 1900.6b. It particularly discusses the developing topics and use cases, and some of the major innovative enhancements and challenges that IEEE 1900.6 is addressing in assisting spectrum databases. Section II of this paper presents a brief introduction of the IEEE 1900.6 standards working group, as well as the key standards that have been and are being developed therein. Section III presents the current thinking on the system model of IEEE 1900.6b and some of the key use cases. Section IV discusses some of the key challenges and current work items of the standard, including some thinking on possible technical solutions for the standard. Section V discusses some detail on a potential technology assessment to verify the 1900.6b approach by an experimental implementation. Finally, Section VI concludes.

II. THE IEEE 1900.6 STANDARDS FRAMEWORK

The IEEE 1900.6 defines spectrum sensing interfaces and data structures for Dynamic Spectrum Access (DSA) and other advanced radio communications systems, providing a standard for the information exchange between spectrum sensors and their clients.

The IEEE 1900.6-2011 baseline standard defines the logical entities and their interfaces, the reference model and its service access points, as well as the service primitives needed to communicate between entities and to utilize their services.

The IEEE 1900.6a-2014 amends the baseline standard by interface enhancements duly considering advanced technology since approval of the baseline standard regarding spectrum sensing and smart sensors. It further elaborates on the data archive entity's functionality and newly includes methods to interface with proprietary (i.e., non-standard, off-the-shelf) spectrum sensors.

IEEE 1900.6b is a recent standards amendment project expected until end of 2017 to submit a standard in particular applicable to a variety of sensing-assisted spectrum database concepts, well in line with ongoing 5G standardization efforts world-wide.

In the course of harmonizing spectrum access in the evolution towards 5G, spectrum sensing also has evolved in significance here being a key technology that complements flexible, software-defined and cognitive radio technologies, and enables communication system concepts that can:

- Rely mainly on spectrum sensing for protecting incumbents from harmful interference;
- Increase availability of wireless communications in difficult or interference-prone radio environments;
- Manage co-existence of heterogeneous wireless systems in dense radio environments.

The 1900.6 is following a technology-agnostic approach that aims not to constrain sensing technology, client design, or type of data link between sensor and client. Nevertheless, due to this evolution more and more communication and database system requirements had to be considered for the standard being of practical vantage for its intended use. One major direction further elaborated down this paper is in the upcoming of concepts for spectrum sensing infrastructures as a service to wireless communication systems implemented as a shared cloud and cloud edge service denoted here as a spectrum sensing infrastructure.

III. IEEE 1900.6 EVOLVED SYSTEM MODEL AND USE CASES

The IEEE 1900.6-2011 baseline standard was drafted according to the general requirements of spectrum sensing likewise covering device-embedded spectrum sensors as well as networks of spectrum sensors. Evolving spectrum-sensing assisted communication and database systems in contrast will emphasize mobile and fixed spectrum sensing infrastructures, blurring further the boundary between spectrum database and spectrum managers. This demand required the 1900.6 working group to consider more deeply the needs of sensing infrastructure's configuration, operations, management and maintenance, and to evolve its system model, use cases, and interface and data structures accordingly.

A. Reference and System Model

Considering system requirements the 1900.6 working group received so far, the IEEE 1900.6b has defined interfaces between a spectrum database and a distributed spectrum sensing system that can be realized by either of two methods:

- As a gateway function hosted by an existing 1900.6 entity such as the Cognitive Engine (CE) or Data Archive (DA) (Fig. 1);
- As a dedicated 1900.6 Spectrum Database (SD) entity that implements the spectrum database functions as a client application to the Application Service Access Point (A-SAP) (Fig. 2).

The latter option is more appropriate to meet stringent communication security and data privacy requirements, while the former is better suited for enhancing an existing spectrum database (or, alternatively, a spectrum manager) application. This option is best chosen if the spectrum database is designed as a cloud-based or similar application and already relies on widely-used protocols from that field.

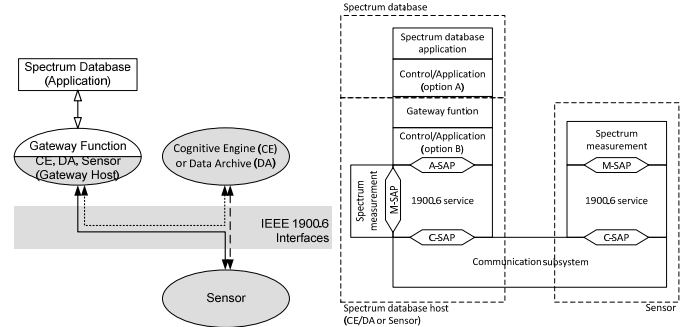


Fig. 1. 1900.6b system model (left) and reference model (right) for a gateway-based spectrum database interface.

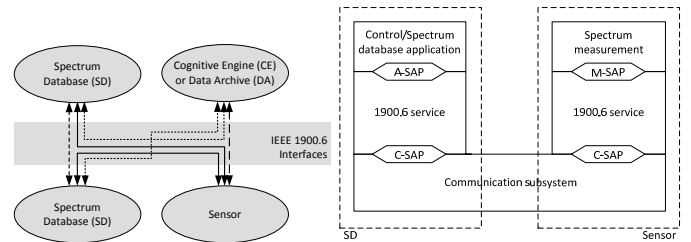


Fig. 2. 1900.6b system model (left) and reference model (right) for a native 1900.6 Spectrum Database (SD) entity.

Future work will further address the exchange of sensing related information between spectrum databases (i.e. 1900.6 SD entities, Fig. 2), which has been identified as a requirement for hierarchical topologies of spectrum databases that may share spectrum sensing infrastructures. A corresponding SD-SD interface has been introduced already by the IEEE 1900.6b.

Following the 1900.6 technology-agnostic approach, the 1900.6b allows an implementation to choose between different communication methods as outlined in Fig. 3 with respect to the model shown in Fig. 1, depending if a spectrum database application wants to access the sensing system through a gateway to the standard A-SAP, by accessing the standard A-SAP or C-SAP directly, by enhancing the 1900.6 services to directly access the Communication Service Access Point (C-SAP), or to apply proprietary communication methods in parallel to the standard SAPs. The latter may be appropriate in case private end-to-end communication must be considered, or dedicated communication sub-system instances are needed for a certain application area. The various methods outlined here can provide different levels of trust and privacy as required.

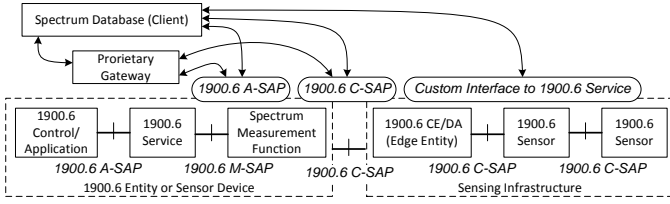


Fig. 3. Communication methods available to a spectrum database application according to Fig. 1 (access through a standard interface, proprietary interface, direct, or through a proprietary gateway and protocol).

B. Major Use Cases

A number of use cases already have been reported earlier [5] and have been further elaborated regarding their particular requirements with regards to interface capabilities, primitive enhancements and data structure modifications needed to support upcoming use cases. Use cases that are currently under review are the following:

- **Wide Area Sensing**, which describes a particular use case for a spectrum sensing-assisted spectrum database derived from the requirements of wide area spectrum management where multiple instances of managed spectrum databases and sensing infrastructures exist in parallel that share information and resources, as well as multiple stakeholders such as authoritative organizations, spectrum owners, infrastructure operators and users.
- **Industrial Communication Sensing**, which describes a particular use case for a sensing-assisted spectrum database derived from the requirements of ultra-low latency and robust industrial wireless aiming to complement wired field-bus communication for implementing industrial process control that involves sensor-actor communication in a real-time control loop.
- **Generic Use Case on Database-Assisted Spectrum Sensing and Message Exchange**, which aims at instantiating the generic use cases for database-assisted spectrum sensing following the guidelines defined in 1900.6 standard and its further amendments. This generic use case could act as the canvas for more specific use case definition and for identification of possible message exchange.
- **Use Cases for Spectrum Database Resource Awareness and Allocation with Aggregation Considerations**, which broadly aim to serve the spectrum database as a resource awareness and allocation tool using information gleaned from sensing, taking into account the possible of aggregating resources appropriately.

IV. IEEE 1900.6B CHALLENGES AND KEY WORK ITEMS

Spectrum-sensing infrastructures, particularly in case of outdoor and wide-area installations but not limited to that, are cost sensitive and demand for solutions that can support multiple concurrent applications. Thus, distinct requirements on the availability and geographical topology of an underlying spectrum sensor network may apply. In particular, it must be possible to manage the network of sensors and its resources,

maintaining availability across periods of rebuild, upgrade or recalibration without degrading its sensing performance. An issue with sensing infrastructure network operations otherwise could result in causing interference by a dependent communication system to an incumbent. The 1900.6 working group analyzed such requirements and agreed in late 2015 upon a number of pressing working items that aim to advance the feature set of service access points, namely the A-SAP and the C-SAP, for addressing these requirements through the upcoming IEEE 1900.6b.

A. Flexibility of Sensing Infrastructures and Topologies

IEEE 1900.6 does not impose any constraints on the geographical or network topology of sensing infrastructures or on the methods used to detect and manage such. But when drafting the standard it was not duly anticipated that environments that need to utilize dense sensor populations or have to observe rapidly changing radio and mobile environments may quickly cause scalability issues due to the communication load on the link between sensors and clients and the number of concurrently reporting spectrum sensors via a shared communication system. In consequence, 1900.6b put some effort on the support of topology management through A-SAP and C-SAP enhancements, without loss of generality enabling the use of multiple communication sub-systems (i.e., enabling multiple C-SAP instances for a 1900.6 entity) and hierarchical topologies (Fig. 4).

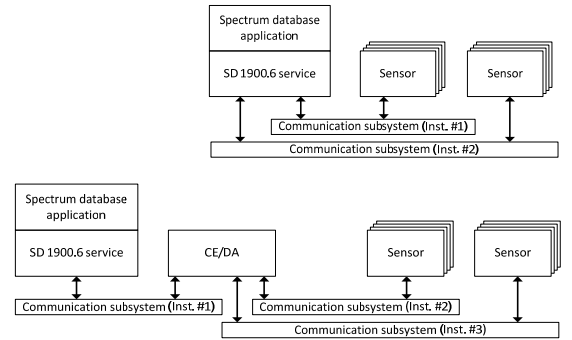


Fig. 4. Spectrum database (1900.6 SD entity) interfacing with 1900.6 Sensor entities through independent communication sub-systems (top), and with independent sensing sub-systems through one or more edge entities (bottom).

Support for compound topologies including (multiple, heterogeneous) localized sensing sub-systems on one hand enables constraining sensing related data traffic to a certain geographical area, potentially coordinating between sensors to remove spatial-temporal redundancy of measurements in that area before communicating that data to the spectrum database, but also imposes addressing constraints and can add single-points-of-failure when using edge entities.

The 1900.6 working group considered this by adding A-SAP and C-SAP primitives and functionality that allows to:

- Create dynamic SAP instances and to assign permanent, temporary, globally unique or scoped identities (i.e., valid only in the scope of a single edge entity) independently from their communication sub-system address (e.g., their IPv4/IPv6 network addresses);

- Access a sensing sub-system through its edge entity or by its individual sensors, if permitted, using network addresses or sensor identities when available;
- Access the same sensor entity through multiple SAP instances, through multiple edge entities, or via separate communication sub-systems, if permitted;
- Assign access policies to a certain SAP instance according to a role model (e.g., user, operator, maintenance, authority...) and to restrict SAP functionality for that role as required;
- Enhance scalability through, e.g., better compression or selective use/forwarding of sensing information achieved by better understanding of spatial, spectral, and perhaps temporal correlation.

Regarding the latter, there are a number of benefits—particularly in contexts such as wide-bandwidth sensing that might otherwise yield a very large amount of data and network load in conveying the resulting information. For example, a mid-point (e.g., a sensor as an aggregation point in a hierarchical collaborative spectrum sensing structure) might assess aspects such as correlation and make the client (e.g., a spectrum database) aware of that. The client then can optimize better how the sensing is performed or which available information is requested or configured and forwarded by the sensors. This could allow for information from only one among a set of correlated sensors (e.g., in similar/nearby radio environments) to be collected/forwarded. Such capabilities might also assist in the frequency domain. In the context of it being ascertained that a number of frequencies all comprise one channel of a radio system through correlation analysis or reporting, using combined measurements from a number of sensors, then only one reading from within that channel would be taken. Supporting this scenario, it is noted that, e.g., in a dynamic spectrum usage case, aspects such as channelization or frequency spacing of systems using the spectrum might not be known to the same extent that they are in conventional (centrally-/regulator-channelized) spectrum usage scenarios.

The above such capacities enable most of the key features outlined next in this section, and will further enable sensing resource management and virtualization of a sensing infrastructure by means of Software Defined Networks (SDN), Network Function Virtualization (NFV) and Network Slicing.

B. Sensing Infrastructure Sharing and Management of Shared Sensing Resources

The capacity to share sensing resources provided by a sensing infrastructure is initially considered by IEEE 1900.6b for the following technical reasons:

- Multiple sensor clients might be interested to observe distinct portions or use objectives of frequency spectrum that a single sensor instance can provide in parallel;
- Multiple sensors can provide the same sensing information enabling operational redundancy in terms of a means to verify measurements, provide a failover path, or for uninterrupted operations during rebuild or maintenance periods;
- A sensor can be part of multiple sensing sub-systems at the same time, potentially representing separated,

purpose-driven geographical topologies, through instantiating distinct SAPs for each of these, covering that it is a shared resource, or controlling its visibility range by using temporal or scoped SAP identifiers;

- A group of sensors, e.g. (dynamically) associated with a dedicated edge element, can provide a separate sensing sub-system that is geographically co-located to another group of sensors or sensing-sub-system, implementing a monitoring function for detecting sensor malfunction or sensor tampering.

In addition, sharing of resources, if sufficiently fine-grained in space, time and function, provides a means to enable network slicing for distributed spectrum sensing infrastructures, which is of particular interest for Mobile Virtual Network Operators (MVNOs) that depend on spectrum databases within their private network slice.

The 1900.6b addresses such resource sharing mechanisms mainly through dynamic SAP instantiation: A temporal A-SAP instance, for example, represents a managed resource that can be further shared in the time domain by periodic locking the SAP instance. As sketched in Fig. 5, shared resources then are (i) sensor instances, (ii) sensor access time slice, (ii) sensing sub-system, while sub-systems are defined by the edge entity (i.e., the CE/DA instance) offering access to the virtual infrastructure of sensors.

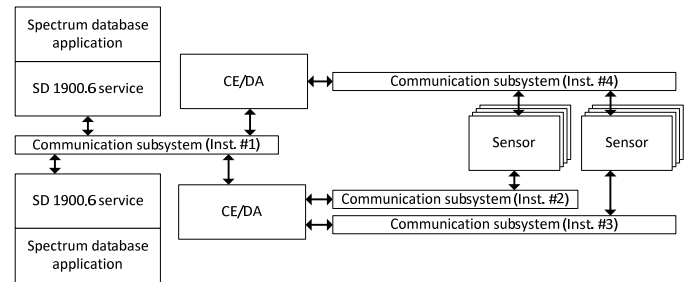


Fig. 5. Sample shared sensing infrastructure scenario.

In such scenario a spectrum database will recognize two distinct sensing sub-systems and may or may not allowed obtaining details on the sensor topology behind, depending on the infrastructure configuration. An edge entity (i.e., the CE/DA) may either disclose or hide sensor SAP identities, the latter being achieved by generating temporal and scoped sensor SAP identities by the edge entity. In consequence, sensor identities would only be available to their associated edge entity as well as their mapping to network addresses. Network access through a communication system in that case can be provided if permitted by Port/Address Translation (PAT/NAT) techniques applied to the sensor network address if any, or to the sensor identity in general.

For certain use cases (e.g., industrial wireless), the ultimate implementation would be to coalesce the functions and entities mentioned above into a single wireless access node (access point, base station, RAN controller...) to obtain a deployable sensing infrastructure.

C. Multi-Tenancy and Sensors Serving Multiple Clients

As with any new technology, it is necessary to achieve a certain market scale or usage base in order for the costs of

development, manufacture, deployment and operational expenditure to be covered by resulting income or otherwise justified. Moreover, sensors might often need to be deployed in difficult-to-reach or protected areas, and only a limited number of locations might be available for the deployment of such sensors and their numbers might need to be limited in certain deployment locations. Given these observations, it will often be of paramount importance for spectrum sensing infrastructures to be available to multiple clients.

In such contexts, the clients will often have very different requirements. For instance, an unlicensed spectrum user (e.g., a Wi-Fi operator employing a spectrum database for management purposes) might wish to use the sensing system merely to assess the likely performance (and optimization) of the selection of particular channels for usage at particular locations, whereas an SAS may use the system (instantiated as an ESC through the ESC meeting the requirements of the 1900.6b specification) to protect vital government capabilities such as radar. Clearly, the latter must have extremely stringent security and reliability constraints to avoid, for example, under all circumstances causing interference with radar return signals or disclosing radar operational parameters, whereas the former might have only very basic such constraints. Moreover, some constraints or configuration settings might be common among the users of the sensing system, allowing those spectrum users to access and use the sensing system under the same configuration at the same time, whereas others might be more specific and unique.

While taking into account such observations, IEEE 1900.6b is enhancing the way in which sensor capabilities are 'locked' by particular clients. This is such that not only will the entire sensor be locked for use exclusively by a client, but specific aspects (e.g., configuration settings) will be able to be locked by/to specific clients while allowing others to vary. This allows clients to access the sensor concurrently, so long as the locked parameters (or conversely, the availability of other parameters for their setting or locking) meet their needs—while maintaining the capability of locking the sensor in entirety to the access by a particular client or clients, if required. Further, 1900.6b considers means for realization of periodic locking of the sensor such that multiple clients can access the sensors in the time domain without interfering.

D. Security and Privacy Enhancements

As with most types of wireless networks, there are numerous security threads that may compromise safety and performance of the system. A scenario where a number of sensors are hijacked or destroyed in order to combine sensing information for pinpointing incumbents cannot be ruled out. Having control over the sensor(s), one can prevent them from acquiring data, or reprogram them to report the wrong data aiming at altering the behavior of the CE / DA for a time period, consequently polluting a spectrum database connected and thus spreading the impact to a much wider domain than the affected sensing sub-system.

Currently, the sensor control and management described in [6], relies on sub-system security lacking an infrastructure-wide security concept. To isolate the rest of the system from potential sensor attacks, a set of entities must be dedicated to offer an extra layer of trust and security between the logical

entities. Through these entities, the sensors should first establish an initial connection by identifying themselves using certificates that can be placed in the firmware of the sensors. As in the case illustrated in Fig. 5, where there are one or more sensing sub-systems, the authentication process of the sensors should be performed through the edge-entities (CE/DA). Sensors are expected to incorporate embedded certificates or for more powerful sensors the credentials could be dynamically exchanged and updated. Once the connection is established with these entities, the sensors will be able to download their configuration and start their operation. Each sensor is expected to contact two entities: one for reporting and one for Updating / Maintenance. These entities can be local or remote and will provide additional security checks. More specifically, the report entity will be used to monitor sensors reading and compare them with other nearby sensors (or itself if as a logical entity features a sensing capabilities) for verification. The update / maintenance entity will be used to occasionally update the sensors security parameters (including certificates) in order to have frequent security checks. Furthermore, these entities will be assigned the role of performing these tasks on a random basis thus preventing attackers from pinpointing them. Another possible scenario is when malicious software (virus) controls the Spectrum Database Application. Infected spectrum database gateway function may provide interfaces and functions to convey false sensing control information. Infected spectrum database gateway function may generate excessive sensing related requests from one or more local or remote sensors aiming at flooding them. The virus propagates from one sensor to the other. In order to avoid this, a sensor should not directly communicate with another sensor without first being verified through an entity that will provide an additional communication link between the sensors. In this case, the virus will be required to break two connections in order to infect more sensors thus providing an extra barrier of security.

E. High-Availability Infrastructures

Spectral efficiency, spectrum sharing and high-availability communications are usually considered conflicting domains. Third tier spectrum users (in order to adopt the related CBRS notation) certainly depend on bilateral agreements with second tiers in order to access spectrum on an exclusive basis. But this will not address the risk of interference caused by non-communication origins such as heavy machinery often encountered for wireless communication in industrial facilities.

Spectrum-sensing assisted databases provide the means to resolve this contradiction at least partially by balancing these on a per-user basis, enabling disclosure of spectral opportunities with least interference probability and categorizing spectrum with respect to its suitability for a particular user and use case.

The IEEE 1900.6b considers such use cases by looking also at hierarchical spectrum database topologies and related spectrum management applications, in particular considering the exchange of sensing information between layers in such a spectrum database hierarchy.

In industrial wireless scenarios, for example, an area or facility-wide spectrum database could be enhanced by local

spectrum databases deployed spatially to industrial processes that use ultra-low latency communication to implement closed-loop sensor-actor interaction sensitive to disruption and latency jitter. Such an approach would allow restricting ‘overbooking’ in the spectral domain (i.e., frequency band reservation for failover in case of ejection from interferers) to locations where this is really needed and would forward spectrum observations also to spectrum databases associated with higher layers in the hierarchy.

Localization of spectrum sensing sub-systems associated with a suitable CE/DA edge entity as outlined above can support high-availability communication finally enhancing the response time of spectrum databases, enabling mobility of spectrum sensing of a sub-system, and would allow more efficient collaboration between sensors (e.g., removing redundancy in local spectrum sensing reports) due to its constrained topology.

V. TECHNOLOGY ASSESSMENT IN 5G EXPERIMENTATION

A growing number of research projects worldwide already conduct experiments on distributed spectrum sensing utilizing federated 5G testbed environments [7], [8]. There is also a growing interest in facilitating such to complement sensing-assisted spectrum databases by spectrum management functions within similar massive machine-to-machine (M-M2M) and Internet-of-Things (IoT) scenarios in the course of 5G related verticals studies.

Consequently, a vital interest for 1900.6b reference implementations exists for several use cases. A first implementation is currently considered for integration with a hierarchical spectrum manager developed earlier, and is considered for deployment as an integrated service of the 5GBerlin trial platform, which is part of the 5GBerlin initiative to enable 5G technology assessment in an urban environment [9], [10], [11]. Further industrial wireless and M-M2M application scenarios are foreseen in this context, in particular addressing spectrum sensing in industrial facilities to assess the potentials and limitations of high availability wireless communications using shared spectrum in dense co-existence and interference-prone environments.

VI. CONCLUSION

The work-in-progress IEEE 1900.6b standard aims to serve a number of compelling cases amending the baseline IEEE 1900.6 standard with specific capabilities around the support for spectrum databases. This paper has highlighted some key aspects of the work towards IEEE 1900.6b, particularly the system model as it is currently seen, some key use cases, and some particular challenges, innovations and enhancements that are being addressed in order to serve spectrum databases with sensing information through IEEE 1900.6b.

Current work in IEEE 1900.6b is particularly addressing the items that have been noted in Section IV of this paper, and also finalizing all system level aspects regarding the reference model described in Section III and in [5], [6]. This includes detail such as: (i) the updates to the Service Access Points and

associated information models supporting the application to spectrum databases, (ii) the enhancement of signaling procedures and the understanding of interface state transitions to support such cases, in addition to refinement of informative content such as the use case descriptions support spectrum databases.

Future work will continue addressing the above-mentioned items, in addition to finalizing aspects of the text input to the standard progressing toward development of the draft. It is currently aimed for the draft standard to be available in 2017.

ACKNOWLEDGEMENT

Bernd Bochow would like to acknowledge the support of the internal projects “FleMMingo – Flexible drahtlose Maschine-zu-Maschine-Kommunikation im industriellen Anwendungsszenario” and “5G Berlin Testfeld – Phase 1 – 5G-Ready Trial Platform”.

Oliver Holland would like to acknowledge the support of an internal Impact Acceleration Award within King’s College London, the Ericsson-King’s 5G Tactile Internet Lab (see, e.g., [12]), the H2020 5G NORMA project, 5gnorma.5g-ppp.eu, and the partial support of the FP7 ICT-SOLDER project, www.ict-solder.eu.

REFERENCES

- [1] FCC, “3.5 GHz Band / Citizens Broadband Radio Service”, accessible at <https://www.fcc.gov/rulemaking/12-354>, Apr. 2015
- [2] GSM Association, “GSMA Public Policy Position: Licensed Shared Access (LSA) and Authorised Shared Access (ASA),” Feb. 2013, accessible at <http://www.gsma.com/spectrum/licensed-shared-access-lsa-and-authorised-shared-access-asa>, accessed Feb. 2015.
- [3] FCC, “In the Matter of Unlicensed Operation in the TV Broadcast Bands, Additional Spectrum for Unlicensed Devices Below 900 MHz and in the 3 GHz Band, Second Memorandum, Opinion and Order,” Sept. 2010 (see also third MO&O from Apr. 2012).
- [4] Ofcom, “Implementing TV White Spaces,” statement, Feb. 2015, accessible at <http://stakeholders.ofcom.org.uk/consultations/white-space-coexistence/statement>, accessed Sept. 2015.
- [5] O. Holland, B. Bochow, K. Katzis, “IEEE 1900.6b: Sensing support for spectrum databases,” IEEE Conference on Standards for Communications and Networking (CSCN 2015), Tokyo, Japan, Oct. 2015.
- [6] IEEE Std 1900.6™-2011, “IEEE Standard for Spectrum Sensing Interfaces and Data Structures for Dynamic Spectrum Access and other Advanced Radio Communication Systems,” Apr. 2011.
- [7] Future Internet Research and Experimentation – FUSION, “Connecting SMEs to the Future Internet”, <http://www.sme4fire.eu>, accessed July 2016.
- [8] NGNM Alliance, “Global 5G Trial & Testing Initiative”, accessible at <https://www.ngmn.org/news/ngmn-news-and-press-releases/ngmn-news-and-press-releases-details/article/ngmn-alliance-pushes-future-focus-areas-with-the-launch-of-the-global-5g-trial-testing-initiative.html>, accessed July 2016.
- [9] B. Bochow *et al.*, “QoS MOS project deliverable D6.5 -- Specification of cognitive and opportunistic functions of the spectrum management framework”, Apr. 2012.
- [10] M. Emmelmann, B. Bochow, “Method for operating a Geolocation Database and a Geolocation Database System”, United States Patent US 9,286,324 B2, May 2016.
- [11] 5GBerlin, “An Initiative for Collaborative Research towards 5G”, accessible at <http://www.5g-berlin.org>, accessed Jul. 2016.
- [12] M. Dohler, “An Internet of Skills...where Robotics meets AI and the Tactile Internet,” IEEE ICC 2016 Keynote Speech, Kuala Lumpur, Malaysia, May 2016. Available at <http://icc2016.ieee-icc.org/content/keynotes>, accessed Jul. 2016.